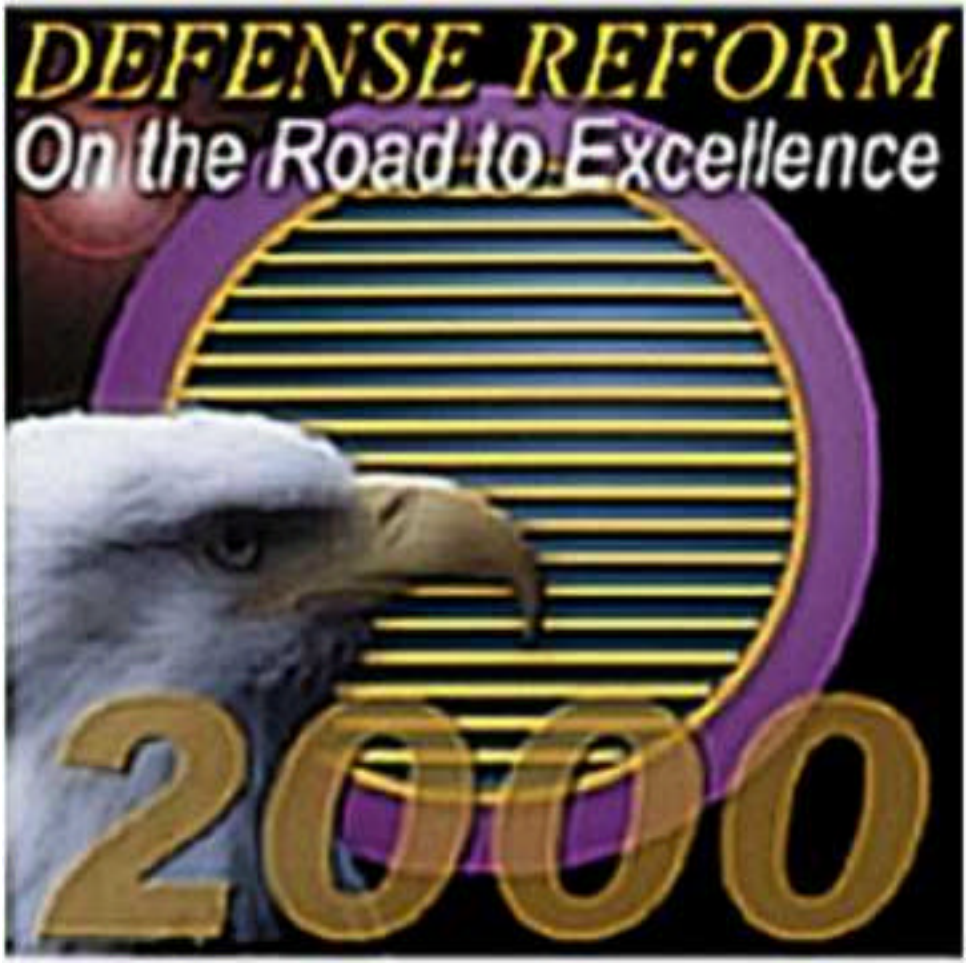

Electronic Commerce Conference

PKI Sub-Group

Issue Paper

INTRODUCTION

The DoD Command and Control Community has certain business models and requirements for the implementation of PKI. Currently, these models drive the requirements of the Business eCommerce PKI Community.

Currently, DoD Command and Control security requirements drive all DoD PKI requirements. These trust models are based upon "Defense in Depth" and other mandates associated with the protection of the DII.

In an electronic commerce/electronic business (EC/EB) PKI based open architecture PKI, the trust models are different. In the commercial marketplace trust based transactions follow a financial model - they have financial value- and are based on actuarial issues and their purpose is the conduct of legally binding transactions over the Internet. There are different trust models between the two domains. We need to better understand the differences and the needs of each.

What is public Key Infrastructure (PKI)?

A PKI is a combination of all the components providing the secure and trusted distribution of public-key encryption and digital signature services. This typically includes integrating digital certificates, public-key cryptography, time stamping, and certificate authorities for enterprise network security infrastructure. Implementing a PKI establishes a trusted networking environment managing encryption keys and digital certificates. It gives and organization the ability to ensure security and integrity of communications and business transactions on the Internet. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

How does PKI Work?

A successful PKI requires trust. Closed PKIs allow an enterprise or "community of interest" (i.e. the DoD Command and Control Community, the medical community, the banking community, etc.) to deploy digital certificates within their own networks. Trust is inherent within closed PKIs.

In order for trust to exist in an open PKI (multiple parties) there must be a trusted third party to vouch for individuals' identities and their relationship to their public keys. In PKI terminology, this entity is referred to as the certification authority (CA).

Why is PKI better than traditional Security Measures?

In electronic commerce (EC), organizations commonly secure the communication medium through the use of private leased lines and networks. For the Internet to offer an inexpensive and ubiquitous solution, the focus must be on information security and identity authentication. The Internet is inherently insecure and there is no way to make it a private environment. In order for the Internet to be used for legally binding transactions, efforts must be directed at securing the message itself- as opposed to the transport mechanism. An effective PKI complements traditional security solutions to offer a more granular and secure solution. A PKI enables secure applications and transactions for many applications. Whether you need virtual private networks (VPNs), e-commerce, secure e-mail, application access security, or Web –based security access control, a PKI can strengthen your existing security. A PKI can also eliminate the issues associated with maintaining different usernames and passwords for application access by allowing Digital Certificate for log on.

In other words, PKI is not a substitute for traditional security measures for protecting networks, it provides additional trust **and is especially useful in providing the additional trust to allow the Internet to serve**

as a vehicle for legally binding EC/EB transactions.

PKI Subgroup of the Security Working Group

This issue paper reports the results and recommendations of the PKI subgroup of the Security Working Group whose membership is listed below.

Rusty Wall- chair - CSC
Ronald A. Martin -Raytheon
Ed Lopez -Cisco
Larry Jewett- Entrust
Joe Mirable- OSD
Michael F. Wells- Microsoft
Christopher O'Connor - elock
William D. Meskill - USAF Staff
Dr. Prakash Ambegaonkar -E-Lock Technologies
Dr. Gene Hilborn -CSC
Louis Jurgens -Digital Signature Trust,Co.
Ketan Mehta -Booz Allen and Hamilton
Thomas L. Hart- GRCI
Jim Litchko -Jim Litchko and associates
Jim Galie -EDS

PROBLEM STATEMENT

Although the benefits of the current DoD PKI program are clear, a review of the DOD Class 4 PKI Architecture Capability Increment 1 (CI-1) reveals that the DOD plan for implementing PKI is to set the bar as high as possible in order to achieve close to DOD Class 4 PKI capability as soon as possible in accordance with the DoD PKI Roadmap.

Additionally, there is no inclusion of DOD Class 2 PKI or provisions for any PKI applications in this program.

The rationale for considering that this is a barrier or a potential barrier to EC/EB is that the objective Class 4 PKI for the security of command and control related applications sets the bar too high for the needs of EB/EC. We believe that this security model will result in higher costs for EB/EC implementations within the DoD and will present a barrier to broad adoption of PKI between the Department and its external trading partners due to these higher costs.

Specifically, the requirement to achieve Class 4 PKI solutions will result in the potential to heighten security requirements for DOD PKI in order to achieve Class 4-like capabilities when many EB/EC applications may only require Class 2 or Class 3 characteristics. The need for commercial entities to achieve Class 3 or 4 capabilities in order to communicate with the DoD will also drive up costs.

Additionally, initial implementation of DoD Class 3 PKI is tied to the success of the common access card. This seems high risk.

DISCUSSION

Within this high level problem statement there were six specific identified PKI-related barriers to eCommerce that are being addressed by the subgroup related to the current implementation of DoD PKI and they are:

1. **Lack of PKI-enabled eCommerce applications and lack of interoperability among PKI applications** - the current program is not focused on providing EC/EB applications that provide utility to the current DoD PKI being implemented. There also are very few current COTS products that are immediately PKI aware. Most PKI alternatives today offer stovepipe alternatives that are based on PKI vendor solutions –not on user community needs. The result is that there is no ease of portability among different vendor solutions and there is no generally accepted principle of one individual having multiple electronic credentials in many different communities. Currently, for example, our wallets contain numerous EC/EB credentials that can be used on hundreds of different applications. The market communities choose the application- we choose the credential and we choose to participate.

2. **DoD is developing a single high assurance PKI** - the current program is focused on satisfying command and control (C2)-based security requirements and, as a result, the security requirements -and associated trust models are focused on satisfying this set of requirements. Associated with this high assurance requirement is the associated requirement to store PKI certificates on common access "smart cards". This presents both a new technology and a potential cost and requirements drivers to the EC/EB community. Associated with this impediment is that DoD is attempting to mandate DoD standards for the commercial marketplace and accordingly is moving to replicate and fund architectures that are already being developed and funded commercially.

3. **Very High Cost Impact to the EC/EB community.** A community that has established but different (perceived to be lower than the C2 community) trust and proofing requirements. Since a single high assurance architecture was chosen for DoD's own PKI, the resultant impact to the EC/EB community if they use these standards to satisfy the requirements for legally binding transactions over the internet will be substantial. This is because commercial EB/EC trust models are not adequate for the needs of the DoD Command and control community. On the other hand, if the DoD chooses to require that the EB/EC community both inside and outside DoD adopt one set of requirements, they will be sufficient for EC/EB but will result in higher costs to all trading partners.

4. **The PKI community lacks metrics for mapping of trust models between the DoD :"high assurance" C2 and EC/EB domains**- there are no current sets of metrics that allow the PKI community to directly map certificate policies for DoD PKI to commercial EC/EB models.

5. **Education of everyone (policy maker through user) to a common level of understanding is a huge challenge.** With the speed of EC/EB technology changes (measured in months not years), the disparate levels of understanding of PKI concepts present barriers within and among user-groups.

6. **While the purpose of using PKI in EC/EB is to provide additional trust to allow the Internet to serve as a vehicle for legally binding transactions, problems still exist with the methodologies associated with establishing a long-term burden of proof.** Specifically, there are no widely adopted industry standards for maintenance of electronic signatures or for authenticated timestamps for record maintenance that have stood the test of time. These processes are untried and the case law has not yet been established to convince users that there are no issues with enforcement of these new processes. An additional barrier to EC/EB within this space is the current DoD Certificate policy in which DoD accepts no liability for these transactions.

Discussion from an EB/EC Perspective

PKI will be especially useful in providing the additional trust to allow the Internet to serve as a vehicle for legally binding EC/EB transactions. In a DoD environment, EC/EB can not be separated completely from the DoD's responsibilities inherent to its mission. Nevertheless a more balanced perspective is necessary to achieve its enterprise EC/EB level goals. Furthermore, after identification and assessment of EC/EB performance drivers and outcomes, the DoD should consider revisiting their requirements in a structured process. This process should include establishing a program focused on developing PKI–related EC/EB internal processes and measures in coordination with both the internal and external EC/EB and PKI industry stakeholders to drive toward the desired EC/EB goals. Fundamentally, the DoD should also consider adopting the best of breed practices in the marketplace.

RECOMMENDATIONS

- Direct DoD CIO to lead a DoD study, with industry participation, to identify opportunities for implementing a more open PKI model that allows operation at multiple assurance levels and report recommendations to the EB Board, by 1 Dec 00.

    - Group to focus on interoperability and application level issues.

    - Explore alternatives to high assurance level defense-in-depth requirements to enhance EB/EC through use of a more applicable PKI class level.

- Direct the DoD CIO, working with the Federal CIO Council and each DoD functional community, to institutionalize within six months partnerships with other federal, state, allied and private sector DoD EB partners to develop mutually acceptable PKI performance metrics, appropriate levels of trust and PKI solutions for core business areas. Further, direct the DoD CIO to request that Industry continue to support an IAWG for formal exchanges with above groups to develop mutually beneficial EB/EC direction.

- Define the EC/EB constituencies. Require that EB/EC business areas examine current DoD and Commercial processes and develop appropriate PKI and trust metrics. Require EB/EC initiatives to establish PKI trust and performance goals and metrics. Derive requirements from overarching best commercial practices.

- Develop requirements for all PKI constituencies - Command and Control related PKI through EC/EB PKI. Develop trust model metrics so that the various EC/EB constituencies can objectively measure levels of trust required for each application.

- Insert business area analyses into evolving DoD PKI Architecture.

- In the areas associated with commercial EC- let commercial practice drive requirements. Examine commercial portable Internet credentials for EC/EB.

- Move to a common EC/EB trust model for all of Federal Government.

- Adopt commercial EC/EB PKI across many applications and utilize commercial trust providers for the purposes of developing metrics and educating users and policy makers - enlist industry to provide com-

mercial PKI trust solutions. A common understanding can be achieved quickly through use and familiarity with the technology.

- Examine COTS alternatives for commercial applications and products that allow users to securely store and easily choose among many PKI certificates.

- Consider moving to an open architecture PKI alternative such as the Civil Government model for EC/EB trust involving Government, industry and citizens-common to all Federal Government. This GSA Program calls for Industry to migrate with Government required changes so change is a part of the current program.

- Utilize commercial EC/EB trust providers. At the end of the day- the EC trust provider has to stand behind its product- assumption of liability- but in a shared liability environment similar to trading partner agreements such as UETA.

IMPLEMENTATION CONCERNS

The vast number of processes and organizations potentially affected by EB/EC would require a significant effort to develop and implement global PKI measures and solutions throughout DoD. Therefore, a more incremental approach is recommended.

Insofar as investment decisions need to be made at the project level, measures should be developed accordingly. In the cases where communities adapt commercial alternatives, they can choose alternatives that allow them to "pay by the drink". The PKI subcommittee therefore recommends that the DoD effort for an objective Class 4 PKI implementation be restricted to the C2 community and that a forum, framework and program be established to examine commercial EC/EB PKI alternatives with funding allocated to use commercial or tailored Government-wide alternatives. This is a policy decision to consider revising the DoD PKI Roadmap for lower assurance levels and more open architectures for EB/EC.

As in all technology implementation, the right balance of integrating multiple data technologies must be achieved with respect to a set of targeted process requirements or the implementation will fail. Employee commitment to new processes will only come about if they believe the new process will allow them to perform their jobs faster or more effectively than a paper based process. Applying measures to the new processes will indicate how well the requirements are being implemented. The most significant measure needed in the PKI space is the ability to compare and contrast trust, security, privacy and other performance requirements using a common set of metrics. The cost per use metric is based upon the marketplace. High use will drive down costs.

With that as a background, today there are also both technical barriers and legal barriers to implementation. Specifically, PKI products and solutions are not sufficiently interoperable with one another to allow plug and play integration and few DoD EC/EB applications are PKI enabled. Within the legal community, trust and legal requirements for EB/EC are currently not well defined or specified.

RESOURCE IMPLICATIONS

Funding for the study is required. There are potential huge savings due to lower assurance requirements that help DoD align with PKI solutions used by private sector and other Federal government agencies. By utilizing

existing PKI solutions, resource costs can be controlled- but project managers should be careful not to invest in duplicating existing commercial architectures and processes. Appropriate assurance levels will also reduce costs for DoD's trading partners and encourage increased participation.